

**PENERAPAN OSSEC SEBAGAI PENDETEKSI INTRUSI PADA WEB
SERVER BERBASIS E-MAIL**

SKRIPSI



disusun oleh

Annisa Rizka Alhimna Rusyda

17.11.1035

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

**PENERAPAN OSSEC SEBAGAI PENDETEKSI INTRUSI PADA WEB
SERVER BERBASIS E-MAIL**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Informatika



disusun oleh

Annisa Rizka Alhimna Rusyda

17.11.1035

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

PERSETUJUAN

SKRIPSI

**PENERAPAN OSSEC SEBAGAI PENDETEKSI INTRUSI PADA WEB
SERVER BERBASIS E-MAIL**

yang dipersiapkan dan disusun oleh

Annisa Rizka Alhimna Rusyda

17.11.1035

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 Juni 2020

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom.

NIK. 190302181

PENGESAHAN

SKRIPSI

PENERAPAN OSSEC SEBAGAI PENDETEKSI INTRUSI PADA WEB SERVER BERBASIS E-MAIL

yang dipersiapkan dan disusun oleh

Annisa Rizka Alhimna Rusyda

17.11.1035

telah dipertahankan di depan Dewan Penguji
pada tanggal 18 November 2020

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Joko Dwi Santoso, M.Kom.
NIK. 190302181

Yudi Sutanto, M. Kom.
NIK. 190302039

Agit Amrullah, S.Kom., M.Kom.
NIK. 190302356

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 15 Desember 2020

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si.,M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 26 November 2020



Annisa Rizka Alhimna Rusyda
NIM. 17.11.1035

MOTTO

“Never stop learning, because life never stop teaching”



PERSEMBAHAN

Saya mempersembahkan skripsi ini kepada semua pihak yang terlibat secara langsung maupun tidak langsung dalam proses pembuatan skripsi.

1. Tuhan Yang Maha Esa yang sudah menguatkan saya dalam menghadapi segala hal.
2. Ibunda drg. Siti Amelia Wardhani dan Ayahanda Ir. Djoni Mudorijanto, yang selalu mendampingi dan memberi pengorbanan baik berupa dukungan moral, material, doa dan kasih sayang tanpa henti kepada penulis.
3. Saudara laki-laki Raden Wildan Faiz Rizkin Adhim dan Muhammad Affan Abdulloh, serta Saudara perempuan Asfarina Zulfa Milata Rosyada, yang selalu memberikan motivasi dan semangat kepada penulis.
4. Bapak Joko Dwi Santoso, M.Kom yang sudah membimbing saya dalam pembuatan skripsi dari awal hingga selesai.
5. Dosen-dosen Universitas AMIKOM Yogyakarta yang telah berbagi ilmu dan pengalaman selama masa perkuliahan.
6. Teman-teman Informatika-02 2017 teman berproses bersama selama kuliah, semoga kita sama-sama menjadi manusia yang bermanfaat.
7. Terakhir, untuk mereka yang tidak bisa disebutkan satu persatu, terimakasih teruntuk siapapun yang tidak pernah mementingkan dirinya sendiri.

KATA PENGANTAR

Puji dan syukur saya panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan kekuatan kepada saya sehingga dapat menyelesaikan skripsi yang berjudul Penerapan OSSEC sebagai Pendeteksi Intrusi pada Web Server Berbasis E-Mail.

Skripsi ini saya buat guna menyelesaikan studi jenjang Strata Satu (S1) pada program studi Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang strata satu dan untuk memperoleh gelar Sarjana Komputer. Dengan selesainya skripsi ini maka pada kesempatan ini saya mengucapkan terimakasih kepada :

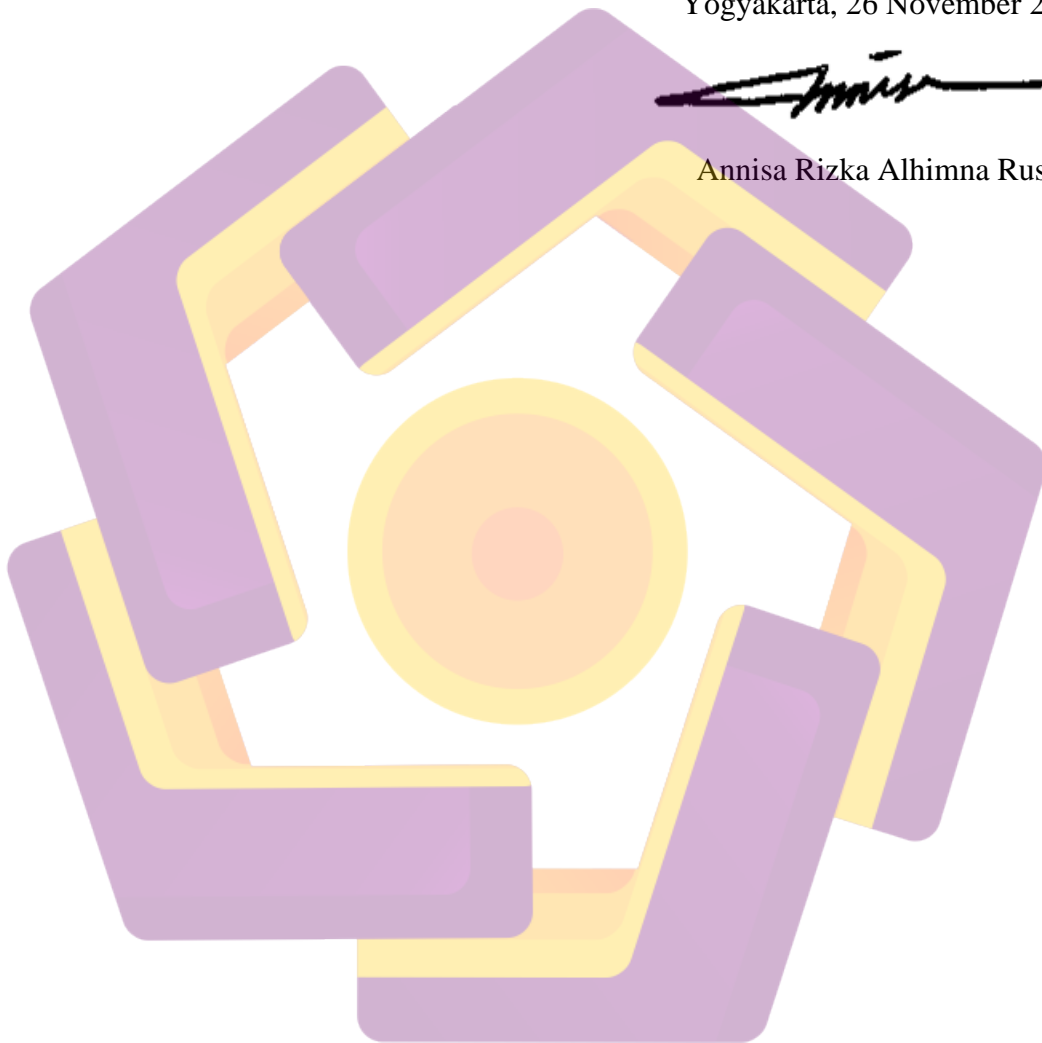
1. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas AMIKOM Yogyakarta
2. Ibu Krinawati, S.Si, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Joko Dwi Santoso, M.Kom. selaku dosen pembimbing yang selalu bijaksana memberikan bimbingan dan arahan selama proses pembuatan skripsi ini.
4. Dosen Penguji (Yudi Sutanto, M. Kom., Agit Amrullah, S.Kom., M.Kom) dan segenap dosen dan karyawan Universitas AMIKOM Yogyakarta yang telah berbagi ilmu dan pengalaman.
5. Kedua orang tua dan keluarga saya untuk doa dan ridho nya.
6. Semua pihak yang sudah memberikan semangat dan membantu dalam proses pembuatan secara langsung maupun tidak langsung.

Semoga Tuhan memberikan kebaikan untuk semua yang telah ikut membantu saya hingga skripsi ini dapat selesai. Demi perbaikan selanjutnya, kritik dan saran yang membangun diterima dengan senang hati. Semoga skripsi ini dapat bermanfaat untuk saya dan kita semua.

Yogyakarta, 26 November 2020



Annisa Rizka Alhimna Rusyda



DAFTAR ISI

PERNYATAAN.....	III
PENGESAHAN	IV
MOTTO	VI
PERSEMBAHAN.....	VII
KATA PENGANTAR	VIII
DAFTAR ISI.....	X
DAFTAR TABEL.....	XIII
DAFTAR GAMBAR.....	XIV
INTISARI.....	XVI
ABSTRACT.....	XVII
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	2
1.3 BATASAN MASALAH	3
1.4 MAKSUD DAN TUJUAN PENELITIAN	4
1.5 MANFAAT PENELITIAN.....	4
1.6 METODOLOGI PENELITIAN	4
1.6.1 Pengumpulan Data	4
1.6.2 Metode Analisis	5
1.6.3 Metode Perancangan	5
1.6.4 Metode Implementasi.....	5
1.6.5 Metode Pengujian.....	6
1.6.6 Analisa Hasil	6
1.7 SISTEMATIKA PENULISAN	6
BAB II LANDASAN TEORI.....	8
2.1 TINJAUAN PUSTAKA.....	8

2.2	DASAR TEORI.....	12
2.3	KEAMANAN JARINGAN.....	12
2.4	DOS (DENIAL OF SERVICE)	13
2.5	DDoS (DISTRIBUTED DENIAL OF SERVICE)	14
2.6	PORT SCANNING.....	14
2.7	OSI LAYER	14
2.8	TRANSMISSION CONTROL PROTOCOL (TCP).....	17
2.9	USER DATAGRAM PROTOCOL (UDP).....	18
2.10	IDS (INTRUSION DETECTION SYSTEM).....	19
2.10.1	NIDS (Network based Intrusion Detection System).....	19
2.10.2	HIDS (Host-based Intrusion Detection System).....	20
2.11	OSSEC	20
2.12	LOIC	23
2.13	POSTFIX	23
2.14	SISTEM OPERASI UBUNTU	23
2.15	WEB SERVER APACHE	24
2.16	NMAP.....	24
2.17	SPDLC (SECURITY POLICY DEVELOPMENT LIFE CYCLE).....	25
BAB III ANALISIS DAN PERANCANGAN		28
3.1	IDENTIFIKASI MASALAH	28
3.2	ANALISIS KEBUTUHAN.....	28
3.2.1	Analisis Kebutuhan Fungsional	28
3.2.2	Analisis Kebutuhan Non-Fungsional	28
3.3	RANCANGAN SISTEM	29
3.3.1	Topologi Jaringan.....	29
3.3.2	Perancangan Sistem Pendeteksi Intrusi.....	30
3.3.3	Perancangan Skema Pengujian	32
3.3.4	Parameter Pengujian Sistem.....	33
BAB IV IMPLEMENTASI		35
4.1	IMPLEMENTASI.....	35



4.1.1	Instalasi Sistem Operasi pada Virtual Machine Server.....	35
4.1.2	Instalasi Sistem Operasi pada Virtual Machine Attacker	38
4.1.3	Instalasi dan Konfigurasi Web Server pada Virtual Machine Server	39
4.1.4	Instalasi dan Konfigurasi OSSEC (Intrusion Detection System).....	40
4.1.5	Instalasi dan Konfigurasi Postfix pada Virtual Machine Server	46
4.1.6	Instalasi Nmap pada Virtual Machine Attacker	50
4.1.7	Instalasi LOIC pada Virtual Machine Attacker	50
4.2	PENGUJIAN.....	51
4.2.1	Pengujian Fungsionalitas OSSEC.....	51
4.2.2	Pengujian OSSEC Server Terhadap Serangan Port Scanning	52
4.2.3	Pengujian OSSEC Server Terhadap Serangan DDoS LOIC.....	55
4.2.4	Pengujian OSSEC Web UI	60
4.2.5	Pengujian Notifikasi E-mail.....	61
4.3	ANALISA HASIL PENGUJIAN.....	63
BAB V KESIMPULAN DAN SARAN.....		66
5.1	KESIMPULAN.....	66
5.2	SARAN.....	66
DAFTAR PUSTAKA		68
DAFTAR LAMPIRAN.....		70

DAFTAR TABEL

Tabel 2. 1 Tabel Penelitian Sebelumnya.....	11
Tabel 2. 2 Model Referensi OSI	16
Tabel 3. 1 Kebutuhan Perangkat Lunak.....	29
Tabel 3. 2 Kebutuhan Perangkat Keras.....	29
Tabel 3. 3 Parameter Pengujian Sistem.....	34
Tabel 4. 1 Pengujian Fungsi pada OSSEC.....	52
Tabel 4. 2 Pengujian Port Scanning	54
Tabel 4. 3 Jumlah Alert Berdasarkan Uji Coba	56
Tabel 4. 4 Jumlah Alert Berdasarkan level	57
Tabel 4. 5 Klasifikasi Alert Berdasarkan level	57
Tabel 4. 6 Jumlah Alert Berdasarkan Rule	59
Tabel 4. 7 Waktu Pengiriman Notifikasi E-mail.....	63

DAFTAR GAMBAR

Gambar 2. 1 OSI Layer	15
Gambar 2. 2 NIDS Monitoring Menggunakan HUB	20
Gambar 2. 3 NIDS Monitoring Menggunakan port SPAN pada Switch	20
Gambar 2. 4 Logo OSSEC	20
Gambar 2. 5 Metode SPDLC	26
Gambar 3. 1 Topologi Jaringan.....	29
Gambar 3. 2 Diagram Alur proses Intrusion Detection System (IDS)	30
Gambar 3. 3 Diagram Alur Perancangan Sistem	31
Gambar 3. 4 Skema Pengujian	32
Gambar 4. 1 Mengunduh File ISO Ubuntu server 16.04	35
Gambar 4. 2 Instalasi Sistem Operasi pada VM Server.....	36
Gambar 4. 3 Tampilan Awal VM Server.....	36
Gambar 4. 4 Konfigurasi IP address, Netmask dan Network	37
Gambar 4. 5 IP Statik	37
Gambar 4. 6 Konfigurasi Jaringan pada VirtualBox.....	38
Gambar 4. 7 Instalasi Sistem Operasi pada VM attacker.....	38
Gambar 4. 8 Instalasi Selesai	39
Gambar 4. 9 Tampilan Web Server Apache	39
Gambar 4. 10 Kategori Instalasi OSSEC	40
Gambar 4. 11 Lokasi Instalasi OSSEC	40
Gambar 4. 12 Notifikasi E-mail OSSEC.....	41
Gambar 4. 13 Integritas Daemon	41
Gambar 4. 14 Deteksi Rootkit.....	41
Gambar 4. 15 Respon Aktif	41
Gambar 4. 16 Respon Firewall-drop.....	41
Gambar 4. 17 White List.....	42
Gambar 4. 18 Remote Syslog	42
Gambar 4. 19 Memulai Instalasi OSSEC.....	42
Gambar 4. 20 Proses Instalasi OSSEC.....	43

Gambar 4. 21 Instalasi OSSEC Berhasil.....	43
Gambar 4. 22 Konfigurasi E-mail notifikasi.....	44
Gambar 4. 23 Konfigurasi Notifikasi File Baru.....	44
Gambar 4. 24 Konfigurasi Real-time Notifikasi	44
Gambar 4. 25 Konfigurasi local rules	45
Gambar 4. 26 Instalasi Web UI OSSEC	46
Gambar 4. 27 Tampilan Web UI OSSEC	46
Gambar 4. 28 Konfigurasi Postfix	47
Gambar 4. 29 Konfigurasi Nama Domain pada Postfix	47
Gambar 4. 30 Konfigurasi SMTP Gmail	48
Gambar 4. 31 Konfigurasi Akun Gmail.....	49
Gambar 4. 32 Email Tes.....	49
Gambar 4. 33 Mengunduh LOIC	50
Gambar 4. 34 Tampilan LOIC	51
Gambar 4. 35 Status OSSEC.....	52
Gambar 4. 36 Pengujian Serangan Ping Attack.....	53
Gambar 4. 37 Mengaktifkan Service OSSEC	53
Gambar 4. 38 Pengujian Port scanning (Quick scan)	54
Gambar 4. 39 Pengujian Port Scanning (Intense scan)	54
Gambar 4. 40 OSSEC Mendeteksi Serangan Port Scanning	55
Gambar 4. 41 Persiapan LOIC	55
Gambar 4. 42 OSSEC Mendeteksi Serangan DDoS.....	60
Gambar 4. 43 Pendeteksian Serangan Port Scanning pada OSSEC Web UI.....	60
Gambar 4. 44 Pendeteksian Serangan DDoS pada OSSEC Web UI.....	61
Gambar 4. 45 E-mail Notifikasi Serangan Port Scanning.....	62
Gambar 4. 46 E-mail Notifikasi Serangan DDoS	62

INTISARI

Keamanan jaringan pada web sever merupakan hal yang harus diperhatikan agar terhidar dari berbagai gangguan yang dapat menghalangi pengguna. Serangan terhadap web server bisa terjadi kapan saja dan dapat mengakibatkan kerusakan data. Penyerangan web server dapat dilakukan dengan berbagai metode salah satunya adalah *Distributed Denial of Service* (DDoS) yang mengirimkan pesan secara terus menerus sehingga dapat mengganggu operasi web server.

Sistem pendeteksi intrusi atau IDS merupakan salah satu metode untuk melindungi web server dari tindakan penyalahgunaan terhadap hak akses ataupun tindakan eksploitasi terhadap keamanan dengan memberikan informasi untuk bersiap dan menangani sebuah serangan yang datang pada web server. Sistem pendeteksi intrusi berbasis host atau HIDS merupakan jenis pertama perangkat lunak pendeteksi intrusi pada web server yang mampu mendeteksi serangan, memantau dan menganalisis serangan pada web server.

Dalam penelitian ini dilakukan pengujian serangan web server yang telah terpasang OSSEC sebagai sistem pendeteksi intrusi pada server linux ubuntu 16.04. Parameter yang digunakan pada penelitian ini adalah jumlah serangan yang dapat dideteksi dan efektivitas dalam mengirim peringatan berupa e-mail kepada administrator jaringan.

Kata Kunci : Keamanan Jaringan, Web Server, IDS, HIDS, OSSEC

ABSTRACT

Network security on web server is important to prevent the number of disruption issues that can interfere the users. Web server attacks can happen anytime and these attacks can cause significant damage to the data. Web server attacks can be done by different methods, one of the most common web server attacks includes Distributed Denial of Service (DDoS), that involves sending large volumes of specific request and causing disruptive impact to the web server operation.

Intrusion detection system or IDS is one of the most effective methods to protect web server from malicious individuals attempting to gain the access rights or exploiting a vulnerability to gain access to sensitive internal information so that the risk of threats to the server can be reduced. Host-based intrusion detection system or HIDS is the first intrusion detection system software to identify potential attacks, includes monitoring and analysis of web server attacks.

Based on this research, the security tests were running by OSSEC as tools of intrusion detection system on linux ubuntu 16.04. server. Parameters that are used on this research including the amount of detected attacks and the effectiveness of recognition in sending e-mail alerts to the network administrator.

Keywords : *Network security, Web Server, IDS, HIDS, OSSEC*